IN THE CLAIMS:

The text of all pending claims, (including withdrawn claims) is set forth below. Cancelled and not entered claims are indicated with claim number and status only. The claims as listed below show added text with underlining and deleted text with ~~strikethrough~~. The status of each claim is indicated with one of (original), (currently amended), (cancelled), (withdrawn), (new), (previously presented), or (not entered).

PENDING CLAIMS

1. (PREVIOUSLY PRESENTED) A data management method comprising:

extracting, as a preview sample, a portion of a digital content file to be distributed;

preparing a substantive file by encrypting the digital content file;

embedding user-specific authorization information, containing information for accessing the encrypted digital content file, as invisible information in the extracted preview sample to prepare user-specific-authorization-information-embedded preview sample;

synthesizing the substantive file and the user-specific-authorization-information-embedded preview sample to prepare a synthesized digital content file ; and

distributing the synthesized digital content file.

2. (PREVIOUSLY PRESENTED) The data management method set forth in claim 1, further comprising:

enabling access to the synthesized digital content file by separating the user-specific authorization information from the preview sample; and

restoring from the user-specific authorization information a decryption key for decrypting the substantive file.

3. (PREVIOUSLY PRESENTED) The data management method set forth in claim 1, wherein the preview sample is image data contained in the digital content file and at least one process among image processing, resizing, compressing and a γ-compensation is executed on the image data.

4. (PREVIOUSLY PRESENTED) The data management method set forth in claim 1, wherein the preview sample is index data for representing the substantive file.

5. (PREVIOUSLY PRESENTED) The data management method set forth in claim 4, wherein the synthesized digital content file contains a plurality of substantive data files based on a plurality of digital content files, and contains a plurality of preview samples corresponding to the plurality of substantive data files; and wherein each preview sample is linked with respective corresponding ones of the plurality of substantive data files.

6. (PREVIOUSLY PRESENTED) The data management method set forth in claim 1, wherein the preview sample is data structuralized in one of JPEG and MPEG formats, and

the synthesized digital content file is prepared by add-on synthesizing the substantive file to the preview sample using the format of the preview sample.

7. (PREVIOUSLY PRESENTED) The data management method set forth in claim 1, wherein the user-specific authorization information is encrypted, and

an encryption key used to encrypt the user-specific authorization information is at least one of user identification information, equipment identification information loaded in user-employed computers, CPU identification information loaded in the user-employed computers, and identification information unique to digital-content-storing recording media.

8. (PREVIOUSLY PRESENTED) The data management method set forth in claim 1, wherein the user-specific authorization information is encrypted, and

an encryption key used to encrypt the user-specific authorization information is identification information common to a plurality of users.

9. (PREVIOUSLY PRESENTED) The data management method set forth in claim

1, wherein the user-specific authorization information is encrypted, and

an encryption key used to encrypt the user-specific authorization information is at least one of identification information unique to distributors of the digital content file, and identification information unique to authors of the digital content file.

10. (PREVIOUSLY PRESENTED) The data management method set forth in claim 7, wherein a decryption key for decrypting the encrypted user-specific authorization information is common to an encryption key for encrypting the digital content file, the decryption key being a shared key based on exclusive information transmitted and received among users and content distributors, using symmetric cryptography.

11. (PREVIOUSLY PRESENTED) The data management method set forth in claim 8, wherein a decryption key for decrypting the encrypted user-specific authorization information is common to an encryption key for encrypting the digital content file, the decryption key being a shared key based on exclusive information transmitted and received among users and content distributors, using symmetric cryptography.

12. (PREVIOUSLY PRESENTED) The data management method set forth in claim 9, wherein a decryption key for decrypting the encrypted user-specific authorization information is common to an encryption key for encrypting the digital content file, the decryption key being a shared key based on exclusive information transmitted and received among users and content distributors, using symmetric cryptography.

13. (PREVIOUSLY PRESENTED) The data management method set forth in claim 7, wherein digital content file distributors encrypt the encryption key employing a secret key, and the users decrypt the encrypted encryption key employing a public key provided in advance from the digital content file distributors, using public key cryptography.

14. (PREVIOUSLY PRESENTED) The data management method set forth in claim 8, wherein digital content file distributors encrypt the encryption key employing a secret key, and the users decrypt the encrypted encryption key employing a public key provided in advance from the digital content file distributors, using public key cryptography.

15. (PREVIOUSLY PRESENTED) The data management method set forth in claim 9, wherein digital content file distributors encrypt the encryption key employing a secret key, and the users decrypt the encrypted encryption key employing a public key provided in advance from the digital content file distributors, using public key cryptography.

16. (PREVIOUSLY PRESENTED) The data management method set forth in claim 1, wherein the preview sample comprises as the invisible information a use count of times a user has used the digital content file; characterized in that the invisible information is rewritten each time a user uses the digital content file.

17. (PREVIOUSLY PRESENTED) The data management method set forth in claim 1, wherein the preview sample comprises as the invisible information authorization information to enable use count control; characterized in that the invisible information is rewritten when a user uses the digital content file a predetermined number of times and more.

18. (PREVIOUSLY PRESENTED) The data management method set forth in claim 16, characterized in that the invisible information is rewritten on decrypting and reading the substantive file.

19. (PREVIOUSLY PRESENTED) The data management method set forth in claim 16, characterized in that the invisible information is rewritten when use of the digital content file is ended.

20. (PREVIOUSLY PRESENTED) The data management method set forth in claim 17, characterized in that the invisible information is rewritten on decrypting and reading the substantive file.

21. (PREVIOUSLY PRESENTED) The data management method set forth in claim 17, characterized in that the invisible information is rewritten when use of the digital content file is ended.

22. (PREVIOUSLY PRESENTED) The data management method set forth in claim 16, wherein the invisible information in the preview sample comprises an error recovery function by containing redundant information.

23. (PREVIOUSLY PRESENTED) The data management method set forth in claim 16, characterized in that limits on read-out and use in decrypting the substantive file are governed based on the invisible information in the preview sample.

24. (PREVIOUSLY PRESENTED) The data management method set forth in claim 16, characterized in that one of year, month, date, and time limits within which read-out and use is possible in decrypting the substantive file are governed based on the invisible information in the preview sample.

25. (PREVIOUSLY PRESENTED) A computer data signal embodied in a carrier wave, comprising protected provider data file synthesized with an extracted accessible sample of the protected provider data file, the sample having watermarked data-authorization information of the provider and data-authorization information of a recipient, thereby allowing a recipient system to preview the protected provider data file via the synthesized extracted accessible sample and access the protected provider data file according to the synthesized extracted accessible sample having the watermarked data-authorization information of the provider and the recipient.

26. (PREVIOUSLY PRESENTED) A computer, comprising:

a programmed computer processor embedding user-specific content-authorization information as a watermark in an extracted accessible sample of a protected content file and synthesizing the extracted accessible sample having the watermarked user-specific-content-authorization information with the protected content file.